# Chapter 3 - Security Education and Awareness

## 301 Security Education and Awareness

A security program is most effective when employees practice security daily. Servicing security officers and security contacts in an operating unit or office will develop, implement, and administer an on-going security education and awareness program for all personnel under his or her jurisdiction. Supervisors are responsible for ensuring that employees fully participate in the program.

**A. Security Education and Awareness Programs.**

1. The security education and awareness program in each operating unit or office should address security in a positive manner. Since many aspects of security apply directly to employees, the heads of operating units and servicing security officers should emphasize an employee's personal responsibilities in proper security practices. These responsibilities include crime prevention and the protection of departmental assets as well as classified information. The servicing security officer should frequently distribute a variety of security information, including posters, videotapes, films, slides, handouts, pamphlets, and computer-based training programs. Law enforcement units from the local community are valuable resources to assist in this effort.

2. The security education and awareness program should include the following elements.

a. Active, continuing participation by each unit's servicing security officer and security contacts.

b. Direction, guidance, and support provided by the head of each operating unit.

c. Security awareness training for all new employees and on-site contract personnel.

d. Periodic security awareness presentations to employees and contractors.

e. Distribution of security reminders such as posters, pamphlets, and checklists.

f. Updated security guidance and directives, as appropriate.

3. The security education and awareness program should include information on recent incidents of security deficiencies or violations, areas of laxity, or trends that have become apparent in the security posture of the operating unit, office, or local facility such as an increase in thefts or security violations.

4. The Security Manual sets standards for the Department's security education and awareness training. Implementation of these standards should:

a. Ensure that each employee who creates, processes, or handles classified information has a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies, procedures, and practices;

b. Increase uniformity among servicing security officers in the conduct of their security education and awareness training activities; and

c. Reduce improper classification, safeguarding, and declassification practices.

**B. Applicability.** The standards pertaining to information security are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to E.O. 12829, the National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions, and safeguards applicable to industry, including security education and awareness training for contractors. The standards established in the Security Manual are consistent with the standards prescribed in E.O. 12958 and the NISPOM.

**C. Responsibility**. The Director for Security has overall responsibility for the Department's security education and awareness program. The servicing security officer of each operating unit and departmental office shall assist the Director in carrying out this responsibility. Servicing security officers must ensure that initial, refresher, and termination security briefings are conducted on a regular basis. Within the first sixty days of employment or appointment with the Department of Commerce, each individual shall attend a general security orientation briefing. An employee who is approved for access to classified information must be briefed on the inherent responsibilities and proper procedures for handling national security information and must execute a Classified Information Nondisclosure Agreement, SF-312, prior to being granted a security clearance. Employees shall be given an annual refresher security briefing within sixty days of their second and subsequent anniversary date of employment or appointment. Upon termination of the individual's security clearance, either by separation, transfer, or change of duties, each employee shall receive a security debriefing explaining the continuing responsibility to protect national security information to which the individual had access.

**D. Approach.** Security education and awareness training should be tailored to meet the specific needs of the Department's security program and the specific role employees are expected to play in that program. The Director shall determine the means and methods for providing security

education and awareness training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods.

**E. Frequency**. The frequency of agency security education and awareness training will vary in accordance with the needs of an organization's security classification program. Each departmental organization shall provide some form of refresher security education and awareness training at least annually for each person who has been granted a security clearance.

## 302 Security Briefings

**A. Coverage.** The Department of Commerce maintains a formal security education and awareness training program that provides for initial and refresher training and termination briefings. This chapter establishes security education and awareness training standards for original classifiers, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These standards are not all-inclusive. The Director may expand or modify the coverage provided in the Security Manual according to program and policy needs. All departmental personnel with a security clearance shall receive initial training on basic security policies, principles, and practices. Such training will be provided in conjunction with the granting of a security clearance, but must be completed prior to an individual being given access to classified information. The following briefings will be required for an employee who has been granted eligibility for access to national security information.

1. **Initial (Entrance-on-Duty) Briefing.** A general security orientation briefing is required for all employees, regardless of their position sensitivity or risk designation, within the first sixty days of employment. This briefing will cover basic security issues such as identification, keys, access control during and after normal work hours, office security and crime prevention, vehicle and visitor controls, property accountability, suspicious package inspection procedures, and emergency evacuation procedures. This briefing must also cover proper usage of information technology. Proper computer and Internet usage must be clearly understood and adhered to by all employees. This briefing can be provided by the operating unit or servicing security officer, a representative from the human resources office, or the employee's first line supervisor.

2. **National Security Education Briefing.** Employees who are approved and cleared for access to classified information must be briefed on their responsibilities with respect to possession of a security clearance and proper procedures for handling national security information. Individuals must execute a Classified Information Nondisclosure Agreement, SF-312, prior to being granted a final security clearance. No individual will have access to classified information until they have received the National Security Education Briefing and they have signed the SF-312. This briefing will include responsibilities of the employee prior

to their transfer, separation, administrative downgrade of clearance, or change of duties and can be conducted by the individual's security contact or servicing security officer. The Office of Security conducts these briefings monthly and accepts all cleared employees. Operating unit security contacts or servicing security officers may schedule cleared employees for this monthly briefing by coordinating directly with the Office of Security.

3. **Annual Security Refresher Briefing.** Annually, employees cleared for access to classified information will receive a refresher briefing covering their security responsibilities. Such employees are required to receive this briefing at least once a year or more frequently, if required. Each operating unit or departmental office may schedule cleared employees for the monthly security briefing provided by the Office of Security.

4. **Information Technology (Computer) Security Briefings.** The proliferation of computers and office automation devices presents vulnerabilities and potential threats to the protection of U.S. Government information. Information Technology security briefings must be provided for all incoming personnel by the Information Technology security staff. This briefing can be incorporated into the initial Entrance-on-Duty Security Orientation Briefing or the operating unit's general office briefing in coordination with Information Technology security personnel. Information relative to computer security (i.e., classified data processing and protection of IT media and passwords) shall be covered in these briefings. IT security briefings must be provided to personnel whose jobs involve processing classified information on a computer system. The Office of Information Technology Management and the Office of Security share responsibility for Information Technology security.

5. **Security Debriefing.** Upon termination of employment or contract responsibilities by separation, transfer, an administrative downgrade action, or a change in duties, each employee or other individual with a security clearance must receive a security debriefing explaining that their access to classified information has been removed and that they have a continuing responsibility to protect national security information. At the security debriefing, each individual shall sign the SF-312 acknowledging the debriefing and their continuing responsibility to protect classified information to which they had access. At a minimum, the debriefing shall contain:

a. A reminder that classified information may not be communicated or transmitted to an unauthorized person or organization;

b. A reminder of the penalty for unauthorized disclosure of classified information;

c. The requirement to report to the Office of Security or to the FBI any attempts by unauthorized personnel to obtain classified information; and

d. The employee's assurance that all classified information has been reassigned to

appropriately cleared personnel in their organization.

**Note: Several servicing security officers have been faced with difficulty in relocating personnel who have transferred, separated, or changed duties. In such instances, the servicing security officer or the security contact shall make every reasonable attempt to locate and debrief these personnel. If such an attempt is unsuccessful, the servicing security officer or security contact shall annotate on the SF-312 that an administrative action was taken on this employee and that the person was not present for the debriefing.**

**B. Special Access Briefings.** Other security briefings will be administered only to those employees who have been cleared for access to special program activities or who require briefings on unique information such as foreign travel advisories. Generally, these briefings are conducted at the Department level or by administrators of the special programs. Employees who no longer have a need for access to a special access program will receive a security debriefing which informs them that access to the special program information has been terminated and that the employee has a continuing responsibility to protect any information to which he or she had access.

1. **NATO Briefing.** The North Atlantic Treaty Organization (NATO) security procedures are contained in the United States Security Authority for NATO Affairs, USSAN 1-69. Before gaining access to NATO information, all Department of Commerce personnel shall be briefed on NATO security procedures. Only an operating unit supervisor, servicing security officer, or other NATO briefed departmental employee may conduct this briefing.

2. **COMSEC Briefing.** Operating unit or servicing security officers shall arrange for individuals who require access to COMSEC information to be briefed on proper COMSEC procedures. A designated COMSEC custodian shall conduct the briefing. Coordination with the Office of Telecommunications Management is required.

3. **Other Special Access Briefings.** Individuals requiring access to Sensitive Compartmented Information (SCI) or Critical Nuclear Weapons Design Information (CNWDI) shall be given a briefing by the operating unit or servicing security officer cleared for these programs. CNWDI policies and procedures are contained in Department of Defense Directive 5210.2. SCI polices are contained in Director of Central Intelligence Directives. For further information concerning special access programs, contact the Office of Security. Not all operating unit or servicing security officers can conduct SCI briefings. SCI access is required for the briefer. If the operating unit or servicing security officer is unable to conduct SCI briefings, he or she should coordinate an appropriate briefing with the Office of Security.

4. **Classification Management Training.** Classification management training is designed

for individuals specifically designated with the authority to make original and derivative classification and declassification decisions. Security officers, classification management officers, security specialists, and other personnel whose duties significantly involve the management and oversight of classified information, must receive classification management training in order to exercise that responsibility. This training shall be accomplished by the operating unit or servicing security officer or can be provided by the Office of Security upon request.

**C. Other Briefings.**

1. **Initial Facility Orientation.** The initial facility orientation briefing will address general physical security principles such as common security hazards, building security, crime prevention, key systems or other site-specific access controls, vehicle controls, property accountability, and package inspection programs. See Appendix L, Sample Memo on Building Security for Employees. Departmental and Federal regulations relating to the handling and safeguarding of classified and sensitive information, including reporting requirements and non-disclosure provisions, must also be covered.

2. **Crime Prevention.** A well-rounded security awareness and education program includes information on crime prevention. Employees should be encouraged to remove or minimize opportunities for crime by being aware of their environment and practicing office security. Employees should also be encouraged to report unauthorized activity, security deficiencies and violations, and safety hazards. Appendix M, Office Security Checklist, and Appendix O, Facilities Security Checklist, provide checklists to assist in determining the adequacy of security in offices and facilities.

3. **Foreign Travel Briefing.** Operating unit or servicing security officers are required to conduct annual foreign travel briefings outlining security and personal safety issues and reporting requirements associated with traveling abroad. This briefing shall be conducted by the operating unit or servicing security officer for employees prior to their foreign travel for the Federal Government. If the operating unit or servicing security officer is unable to provide an oral briefing, the written Defensive Foreign Travel Briefing will be made available to the traveler.

4. **Counterintelligence Briefing.** Operating unit and servicing security officers are required to conduct counterintelligence (CI) briefings to educate personnel about foreign intelligence threats and foreign contact reporting procedures. This briefing shall be incorporated into the Initial Entry-on-Duty Security Orientation Briefing and be repeated during the Annual Refresher Briefing.